AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Ronald Morin, a Special Agent with the United States Department of Homeland Security ("DHS"), Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI"), being duly sworn, depose and state as follows:

1. I have been employed as an HSI Special Agent since May of 2006, and am currently assigned to the Manchester, New Hampshire Resident Office. Prior to my employment with HSI, I served as a Police Officer in the State of Maine. As part of my regular duties as a Special Agent, I am tasked with the investigation of criminal violations related to child exploitation and child pornography, including violations pertaining to the illegal transfer of obscene material to minors, in violation of 18 U.S.C. Section 1470 and possession of child pornography, in violation of 18 U.S.C. Section 2252(a)(4)(B) (the "Specified Federal Offenses"). I have received training in the area of child pornography and child exploitation, and as part of my duties have observed and reviewed examples of child pornography (as defined in 18 U.S.C. Section 2256) in various forms of media, to include digital/computer media. During the course of this investigation I have conferred with other investigators who have conducted numerous investigations and executed numerous search warrants which involved child exploitation and/or child pornography offenses. I have previously obtained federal search warrants related to child pornography offenses and have participated in the execution of numerous search warrants, many of which involved child pornography offenses.

2. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

3. This affidavit is made in support of an application for a search warrant authorizing a search of Matthew Perkins's ("PERKINS") residence, located at 54 Newton Junction Road,

Kingston, New Hampshire 03848 (the "Premises"), his registered vehicle, a silver 2007 Ford Freestyle van bearing New Hampshire license plate 4361017, with a vehicle identification number of 1FMDK05177GA00653 (the "Vehicle"), and his person, as further described in Attachments A and B, as applicable. Located within the Premises and the Vehicle to be searched, I seek to seize evidence, fruits, and instrumentalities of the foregoing criminal violations, which relate to the knowing transfer of obscene material to minors and possession of child pornography. I request authority to (i) search the entire Premises, including the residential dwelling and detached garage, the entire Vehicle, his person, and any computer and computer media located therein and where the items specified in Attachment B may be found; (ii) seize from the Premises and the Vehicle any and all items listed in Attachment B as instrumentalities, fruits, and evidence of the Specified Federal Offenses.

4. The statements in this affidavit are based in part on information provided by other law enforcement officers, and on my own investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of the Specified Federal Offenses are presently located at the Premises, in the Vehicle, or on the person of Matthew PERKINS.

5. The first section of this affidavit recites the statutory language and definitions for the relevant Specified Federal Offenses. The second section of the affidavit provides background on computers and child pornography in general and details the specifics of search and seizure of computer systems. Finally, the third section of the affidavit provides the probable cause to believe that (i) the Specified Federal Offenses have been committed; and (ii) that the evidence,

fruit, and instrumentalities of the Specified Federal Offenses are likely to be found in the Premises and the Vehicle, and on Matthew PERKINS's person, respectively.

SECTION I. STATUTORY LANGUAGE AND DEFINITIONS

A. STATUTORY AUTHORITY

6. This investigation concerns alleged violations of 18 U.S.C. Section 1470 relating to the transfer of obscene material to minors. The relevant statute is recited in pertinent part as follows: "Whoever, using the mail or any facility or means of interstate or foreign commerce, knowingly transfers obscene matter to another individual who has not attained the age of 16 years, knowing that such other individual has not attained the age of 16 years, or attempts to do so, shall be fined under this title, imprisoned not more than 10 years, or both."

7. This investigation also concerns alleged violations of Title 18, United States Code, Section 2252(a)(4)(B) relating to the possession of child pornography. 18 U.S.C. § 2252(a)(4)(B) states that it is unlawful for any person to knowingly possess, or knowingly access with intent to view, one or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct, and such visual depiction is of such conduct.

B. DEFINITIONS

8. The following definitions apply to this Affidavit and Attachment B:

a. "Child Pornography" includes any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct where (A) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (B) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (C) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. Section 2256(8).

b. "Computer" refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." *See* 18 U.S.C. Section 1030(e)(1).

c. "Computer hardware" consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

d. "Computer passwords and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

e. "Computer-related documentation" consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

f. "Computer software" is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. "Minor" means any person under the age of 18 years. *See* 18 U.S.C. Section 2256(1).

h. "Sexually explicit conduct" applies to visual depictions that involve the use of a minor, *see* 18 U.S.C. Section 2256(8)(A), or that have been created, adapted, or modified to appear to depict an identifiable minor, *see* 18 U.S.C. Section 2256(8)(C). In those contexts, the term refers to actual or simulated sexual intercourse (including genital-genital, oral-genital, or oral-anal), whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic areas of any person. *See* 18 U.S.C. Section 2256(2)(A).

i. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image; and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. *See* 18 U.S.C. Section 2256(5).

j. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); mechanical form (including, but not limited to, phonograph records, printing, typing); or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMCs"), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

SECTION II. BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY; SPECFICS OF COMPUTER SEIZURES

A. BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

9. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers, computer technology, and the Internet have revolutionized the manner in which child pornography is produced, possessed, and distributed.

10. Computers basically serve five functions in connection with child pornography: production, communication, distribution, storage, and social networking. With digital cameras, images of child pornography can be transferred directly onto a computer; in addition, the use of commercially available software and devices also allows for the conversion and transfer of other forms of visual media into various digital and electronic media formats. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to millions of computers around the world.

11. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

12. The Internet affords individuals several different venues for meeting and communicating with each other; and obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. The Internet is also used as a means for child sexual exploitation offenders to solicit potential victims through the use of various online services to include, but not limited to, online profiles, email, and instant messaging and chat.

13. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP (Internet Service Provider) client software, among others. In addition to electronic

communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space -- that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space -- for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

14. File transfers and online connections occur to and from IP (Internet Protocol) addresses. These addresses, expressed as four sets of numbers separated by decimal points, are unique to particular computers during online sessions. An IP address identifies the location of the

computer with which the address is associated, making it possible for data to be transferred between computers.

15. Third-party software is available to identify the IP address of a particular computer during an online session. Such software monitors and logs Internet and local network traffic. It is possible to identify the person associated with a particular IP address through ISP records. ISPs maintain records of the IP addresses used by the individuals or businesses that obtain Internet connection service through the ISP. Those records often include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, and other information both in computer data and written record format.

B. SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

16. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish fully on-site.

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific

> procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

17. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit ("CPU"). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

18. Furthermore, because there is probable cause to believe that the computer and its storage devices are all instrumentalities of crimes, within the meaning of 18 U.S.C. Sections 1470 and 2252, they should all be seized as such.

SECTION III. PROBABLE CAUSE

19. On July 4 2018, Interpol in Washington, DC received the following information from Interpol in Manchester, United Kingdom. On Monday April 23, 2018, an 11-year-old female received a contact (likely a follow request) from Instagram account "joeygo12345" on her Instagram account. The victim initially thought this was a Joey that she knew, so she accepted his contact. Over the next 24 hours, the "joeygo12345" account began a sexual discussion with the child and sent her a picture of an erect penis and a video of a male masturbating.

20. The victim sent a message threatening to report the offender to the police, and he then stopped contacting the victim. The offender then blocked the victim on Instagram. The victim disclosed the incident to her school teacher who referred the matter to the police.

21. The UK authorities took screen shots of the conversations on the victim's phone and provided me with a transcript of the conversation at issue which I have reproduced below. I also reviewed the photograph associated with the victim's Instagram account which clearly depicts a minor female. Anyone who communicated with the victim on Instagram would have clearly observed her profile photograph when communicating with her. The conversation is as follows. "SUSPECT" represents the user account "joeygo12345."

SUSPECT: Hey Cutie
VICTIM: Who is this?

DATE/TIME: 04/23/2018 at 22:48 (GMT)
SUSPECT: I just think you are hot
SUSPECT: Is that ok

DATE/TIME: Yesterday at 00:41 (GMT)
VICTIM: No no it isn't
VICTIM: It's weird and I don't even know me

DATE/TIME: Yesterday at 11:44 (GMT)
SUSPECT: Yea keep it up I will show you my cock
SUSPECT: And I will show you me cumin
SUSPECT: Do you
VICTIM: How old are u??
SUSPECT: Do you like to see Dick
VICTIM: Who is this
SUSPECT: Do you
VICTIM: Who is this and how old are u??
SUSPECT: How old are you
SUSPECT: 15
VICTIM: Okay now what's ur name
SUSPECT: Want to see my Dick
VICTIM: What ur name
SUSPECT: Ok you don't want to see it
VICTIM: Do you live in England??
SUSPECT: Have you seen Dick
VICTIM: No
SUSPECT: Want to
SUSPECT: On what
VICTIM: What school do u go to
SUSPECT: I'm just not going to show you

SUSPECT: Ok
VICTIM: Okay

At this point in the conversation, the joeygo12345 account sent a still image depicting an adult Caucasian male wearing a long sleeve red/black flannel with a white/black draw string with an exposed erect penis. The male appears to have pubic hair. Only a portion of the male's neck is visible. His face is not visible.

SUSPECT: Do you like that
VICTIM: U don't look 15
SUSPECT: I am so you don't like Dick
SUSPECT: What does
SUSPECT: Do you know we're the dick would go in you
SUSPECT: Haha can I see that pussy
SUSPECT: Have you seen Dick before
VICTIM: Umm?
SUSPECT: Have you seen a man cum before
VICTIM: No
SUSPECT: Want to
SUSPECT: Yea or no
VICTIM: This is awkward
SUSPECT: So no
SUSPECT: Yea or no
SUSPECT: So no
VICTIM: Ummmm
SUSPECT: Just say no or yes
SUSPECT: What
SUSPECT: So do you or no

The joeygo12345 account then sent a video depicting an adult Caucasian male holding his exposed penis in his right hand, masturbating.

SUSPECT: Tell me if you like that and want more
SUSPECT: Like it
SUSPECT: Want more
SUSPECT: Ok sorry have a good day

DATE/TIME: Yesterday at 14:50
SUSPECT: Like it
SUSPECT: Want more
VICTIM: No I don't want more
SUSPECT: You did not like
VICTIM: No I didn't do now if u didn't mind leave me alone
SUSPECT: Y you like pussy
SUSPECT: I will make you suck my Dick

VICTIM: Nah just go away leave me alone and just go away or else I will report you to the police and you will go to jail
VICTIM: No I don't want more
VICTIM: Seriously
VICTIM: Leave me alone

22. The UK authorities received business records from Instagram for the account with username "joeygo12345" indicating that it was registered on March 26, 2018, at 22:44:14 (UTC) with the name "Joe" and was verified with telephone number [redacted]1765 ("the 1765 Phone"). The records indicated that the joeygo12345 account was registered on March 26, 2018, from IP address 2601:18a:9327:24e2:d29c:7843:6a5a. A DHS Summons to Comcast for the IP address on the registration date and time showed that it was registered to Matthew Penkins, 6 Laurel Lane, Apartment B, Georgetown, Massachusetts, with telephone number [redacted]5376. Georgetown Police have associated the 5376 Phone with PERKINS. It had an associated email user ID of "laureljoe." PERKINS's parents reside at 6 Laurel Lane, Apartment B, Georgetown, Massachusetts.

23. Consolidated Lead Evaluation and Reporting (CLEAR) database records associated the 1765 Phone number with a Matthew PERKINS, 64 Elm Street, Apartment A, Georgetown, Massachusetts. This telephone was also associated, by the Georgetown Police Department, with PERKINS's wife, Kerry Ann Perkins. On September 19, 2018, SA Morin issued a DHS Summons to TracFone Wireless for subscriber information on the 1765 Phone which indicated that the phone was in service and subscribed to Kerry Kerkeeins from Georgetown, MA from January through September of 2018. I note that Kerkeeins when pronounced phonetically, sounds like Perkins. On the same day that service ended in September, service began with Comcast for the same phone number. Comcast records indicate that the phone was subscribed to Kerry Perkins of 54 Newton Junction Road, Kingston, New Hampshire (the Subject Premises).

24. The Georgetown, Massachusetts Police Department confirmed that PERKINS used to live in Georgetown at 64 Elm St., Apartment A. In August of 2017, the Georgetown Police learned that although the children were attending school in Georgetown, the family may have moved out of the town. Georgetown officers spoke to PERKINS who said he was currently living at a church in Plaistow, New Hampshire but that he considered his family homeless. In December of 2017, the Georgetown Police spoke to him again and he said that while he was still residing at the church in Plaistow, he was soon moving to the Subject Premises in Kingston, New Hampshire.

25. The Kingston, New Hampshire Police confirmed that PERKINS moved to the Subject Premises by at least March of 2018 and that he still resides there with his wife, Kerry Perkins, three daughters (the oldest of which is about thirteen years old) and newborn son. In addition, the Kingston Police believed another adult female may reside there as well. I confirmed that the Subject Premises is the registered address of PERKINS and his wife.

26. On November 30, 2018, United States District Judge Andrea K. Johnstone issued a search warrant for records from the joeygo12345 Instagram account. On December 14, 2018, SA Morin received 752 pages of Instagram Business Records from Facebook/Instagram for Instagram user account "joeygo12345." The records indicate that the account was disabled on May 28, 2018, at 15:23:05 UTC.

27. The records contain communications from the date the account was activated, March 27, 2018, through May 26, 2018. The communications are almost exclusively with females and are sexually explicit. In most conversations, the user joeygo12345 sent images of a man's penis to others. Many of the conversations make clear that joeygo12345 is targeting minor child victims and he frequently requests that they send him sexually explicit pictures of themselves.

28. For example, between May 14, 2018, and May 16, 2018, Instagram user "joeygo12345" engaged in sexually explicit communications with Instagram user "[redacted]." "Joeygo12345" asked, "how old are you…how many D have you seen…have you had sex?" The child responded, "14." Through several texts, "joeygo12345" asked "do you like big D or small or average…if you want to see mine let me know." The female asked, "so how old are you." "Joeygo12345" responded, "I'm too old for you…what do you want to do to a D…OK so never seen a D cum…have you played with yourself before…you like it…cool do you want to have sex…I'm so hard I want more pics of you." Eventually the child asked if he had Snapchat and he responded in the affirmative. "Joeygo12345" asked the female "you going too send me something…pussy feet…please I'm so horny." The child responded that she was at school in Massachusetts. "Joeygo12345" instructed the female to go into the bathroom at school to send him something. The female responded, "Boom, now ur turn" as if she had sent something. This file is not included in the Instagram records provided and may have been sent over Snapchat. I believe, therefore, that the minor female may have sent a sexually explicit photograph to the joeygo12345 user.

29. I was able to identify the minor child who used the Instagram account discussed above and confirmed that she is a 14-year-old child with ties to Georgetown, Massachusetts, where PERKINS previously lived.

30. I identified at least two other children who had similar conversations with the joeygo12345 account. One was a minor who also had ties to Georgetown, Massachusetts. Another was a 14-year-old female from Fitchburg, Massachusetts. In another conversation, "joeygo12345" sent a close up picture of a vagina to another person he was communicating with

on Instagram. Although it is hard to tell with certainty, based on the structure and lack of pubic hair, I believe that the picture may be of a minor female.

31. In some conversations, the "joeygo12345" account user presents him or herself as a female. In others, he or she presents as a male. During two conversations, the account sent pictures purporting to be of himself that show more than just his penis. Neither of those photographs depict PERKINS. Only one shows a face. I have been unable to identify the person depicted in the photograph. Based on my training and experience, I know that people who do illicit things on the internet often try to disguise their identity. In addition, when people engage in sexually explicit conversations with children, they frequently pretend to be younger or more attractive in order to appear more desirable to their targets.

32. Instagram user "joeygo12345" sent media files of an adult Caucasian male with an erect penis exposed using IP Address 24.91.213.184 to four other Instagram users (all appear to be females) on separate occasions. This IP address is subscribed at the Subject Premises. In fact, as recently as December 21, 2018, I subpoenaed information from Comcast about the subscriber for the account at the Subject Premises. Comcast confirmed that the IP address was 24.91.213.184 subscribed to Kerry Perkins at the Subject Premises with associated telephone numbers [redacted] 2672 and the 1765 Phone.

33. On December 27, 2018, I called the 1765 Phone and a male answered. The Sanborn Regional School District had the 1765 Phone on record as the phone number associated with the emergency contact for the Perkins children (along with an email address for Matthew PERKINS).

34. New Hampshire DMV records also identified that PERKINS has a silver 2007 Ford Freestyle bearing New Hampshire license plate 4361017, registered to him at the Subject

Premises. On September 17, 2018, November 28, 2018, and January 8, 2019, law enforcement officers observed the Vehicle at the Subject Premises.

35. Because the joeygo12345 account was opened with an IP address associated with PERKINS's parents' address, and accessed from his Kingston, New Hampshire address after he moved there, and because it was verified with the 1765 Phone, associated with PERKINS and his wife, I think there is probable cause to believe that PERKINS used the joeygo12345 Instagram account.[1]

36. Although the account closed in May, I believe that evidence of the conversations at issue may still be present on electronic devices in the residence. As I believe the user of the account has a sexual interest in children and at least attempted to have various children send him sexually explicit images of themselves, I believe that evidence of these images may still be on the electronic devices in the residence. I know, based on my training and experience, that individuals with an interest in child pornography tend to collect and save it for long periods of time. They may do so on telephones, computers, flash drives, and other electronic devices discussed in this affidavit. Even if they do attempt to delete these photographs or evidence of internet accounts they previously used, forensic examiners can often recover deleted information that would provide evidence of the crimes discussed herein.

CONCLUSION

37. Based on the aforementioned facts and circumstances, your Affiant respectfully submits that there is probable cause to believe that Matthew PERKINS, who resides at the Premises and operates the Vehicle, has violated the Specified Federal Offenses; and that the fruits, evidence,

[1] Although investigators received additional IP addresses from Instagram, most of them were dynamic, which means that they would not likely allow me to identify a location of the login. However, I received subscriber information for one other IP address that was not dynamic that was subscribed in the name of Saundra Winer at 7 Pleasant Street, Unit B in Georgetown, Massachusetts. This address is not associated with PERKINS but may indicate that the joeygo12345 account logged in to the internet at that residence on at least one occasion.

and instrumentalities of the Specified Federal Offenses are likely to be found at the Premises, the Vehicle, and on Matthew PERKINS's person.

38. Your Affiant, therefore, respectfully requests that a search warrant be issued authorizing the search of the Premises, Vehicle, and/or person of Matthew PERKINS listed in Attachment A and the seizure of the items listed in Attachment B.

/s/ Ronald Morin
Ronald Morin
Special Agent
U.S. Department of Homeland Security
Immigration and Customs Enforcement
Homeland Security Investigations

Sworn and subscribed before me this 16th day of January, 2019.

/s/ Andrea K. Johnstone
HONORABLE ANDREA K. JOHNSTONE
UNITED STATES MAGISTRATE JUDGE
DISTRICT OF NEW HAMPSHIRE

ATTACHMENT A

DESCRIPTION OF THE PREMISES

The residence is a beige/wood single family one story ranch style home with a detached one car garage. There are two bedrooms, one bathroom, and 1203 sq. ft. of living space. The residence is beige with white trim around the windows and front door. The entry door is white and located on the driveway side of the structure. The numerals "54" are affixed to the mailbox at the roadway and on the telephone pole in front of the residence. The detached garage is gray with a white entry door. (the "Premises").

ATTACHMENT A

DESCRIPTION OF THE VEHICLE

The gray 2007 Ford Freestyle van bearing New Hampshire license plate 4361017, with a vehicle identification number of 1FMDK05177GA00653, registered under the name Matthew Walter Henry PERKINS as depicted below in front of 54 Newton Junction Road, Kingston, NH (the "Vehicle").

ATTACHMENT A

DESCRIPTION OF THE PERSON

The person of Matthew Walter Henry PERKINS, with an address of 54 Newton Junction Road, Kingston, New Hampshire 03848 (social security number 017-xx-xxxx, and year of birth 1982), height 5’09”, weight 190, hair brown, and eyes brown, as described in his New Hampshire Driver’s License.

ATTACHMENT B

ITEMS TO BE SEARCHED AND SEIZED

Electronic and other communications pertaining to the solicitation, enticement, coercion, persuasion, inducement, and sexual exploitation of a minor and images of child pornography and files containing images of child pornography in any form, wherever these items may be stored or found including, but not limited to:

1. Any computer equipment, computer, computer system and related peripherals, tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drive and other computer-related operation equipment, cellular phones, digital cameras, video cameras, scanners, computer photographs, graphic interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG), and any electronic data storage devices including, but not limited to, hardware, software, diskettes, backup tapes, CD-ROM's, DVD's, flash memory devices, and other storage mediums; any input/output peripheral devices, including but not limited to passwords, data security devices and related documentation, and any hardware/software manuals related to or used to visually depict child pornography or child erotica; contain information pertaining to the interest in child pornography; and/or distribute, receive, or possess child pornography, and child erotica or information pertaining to an interest in child pornography, child erotica or information pertaining to an interest in child pornography or child erotica;

2. Books and magazines containing visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. Section 2256;

3. Originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. Section 2256;

4. Motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. Section 2256;

5. Information, electronic records, or correspondence pertaining to the possession of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. Section 2256, that were transmitted or received using computer, some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:

a. registries regarding peer-to-peer file-sharing software communications and participants in peer-to-peer file-sharing software networks;

b. envelopes, letters, and other correspondence including, but not limited to electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. Section 2256; and

c. books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. Section 2256;

6. Credit card information including but not limited to bills and payment records;

7. Records evidencing occupancy or ownership of the Premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence, and/or ownership of the Vehicle;

8. Records or other items that indicate ownership or use of computer equipment found in the Premises and/or Vehicle, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes;

9. Records, electronic or otherwise, or other items that relate to internet accounts and usernames, or any other groups that exhibit a sexual interest in children;

10. Contraband, the fruits of crime, or things otherwise criminally possessed, or property which is or has been used as the means of committing the foregoing offenses;

11. Evidence of sending sexually explicit material to children including sexually explicit material of adults, sexually explicit communications with children, and clothing that appears to be depicted in the explicit images sent from the joeygo12345 account to others over Instagram.

DEFINITIONS

For the purpose of this warrant:

A. "Computer equipment" means any computer hardware, computer software, computer-related documentation, storage media, and data.

B. "Computer hardware" means any electronic device capable of data processing (such as a computer, personal digital assistant, cellular telephone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical

locks and keys).

C. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

D. "Computer-related documentation" means any material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

E. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, USB or thumb drive, or memory card).

F. "Data" means all information stored on storage media of any form in any storage format and for any purpose.

G. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.

RETURN OF SEIZED COMPUTER EQUIPMENT

If, after inspecting seized computer equipment, the government determines that the equipment does not contain contraband or the passwords, account information, or personally-identifying information of victims, and the original is no longer necessary to preserve as evidence, fruits or instrumentalities of a crime, the equipment will be returned within a reasonable time, if the party seeking return will stipulate to a forensic copy's authenticity (but

not necessarily relevancy or admissibility) for evidentiary purposes.

If computer equipment cannot be returned, agents will make available to the computer system's owner, within a reasonable time period after the execution of the warrant, copies of files that do not contain or constitute contraband; passwords, account information, personally-identifying information of victims; or the fruits or instrumentalities of crime.